UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

---------- x

MICHAEL SCHILLER, et al.,

Plaintiff,

DECLARATION OF BRIAN M. JENKINS

-against-

THE CITY OF NEW YORK, et. al,

Defendants.

04-Civ-7922 (RJS)(JCF)

---------- x

CONSOLIDATED RNC CASES

(RJS)(JCF)

---------- x

BRIAN M. JENKINS, declares under penalty of perjury and pursuant to 28 USC § 1746, that on the basis of personal knowledge and upon a review of the selections of the record provided to me that the following statements are true and correct:

1. I submit this declaration in support of Defendants' motion for summary judgment and to set forth my expert opinion that the policy implemented by the New York City Police Department (the "NYPD") that individuals engaged in criminal conduct related to the 2004 Republican National Convention (the "RNC") were to be fingerprinted as part of their arrest processing (the "Fingerprinting Policy") was both appropriate and a best practice for an event like the RNC.

My Qualifications

2. I have been involved in security matters for more than forty ("40") years. In 1962, I was commissioned as an officer in the U.S. Army, subsequently serving in Latin

America and Southeast Asia. While in the Army, I became a paratrooper and ultimately a Captain in the Green Berets. I am a decorated combat veteran, served in the Special Forces Group and was a member of the Long Range Planning Task Group in Vietnam in 1968 and 1969. In 1969, I received the Department of the Army's highest award for my service.

3. Following military service, I joined the RAND Corporation and initiated its research program on terrorism in 1972. The RAND Corporation is a nonprofit institution that helps improve policy and decision making through research and analysis. RAND focuses on the issues such as health, education, national security, international affairs, law and business, and the environment. From 1972 to 1989, I directed RAND's research on political violence.

4. From 1989 to 1998, I was the Deputy Chairman of Kroll Associates, an international investigative and consulting firm. At Kroll, I was responsible for the firm's crisis management practice and directed the responses to kidnapping and extortion cases worldwide.

5. I also served as an advisor to the Los Angeles Olympics Organizing Committee on matters pertaining to security in 1984. Since 2003, I have also unofficially advised the New York City Police Department (the "NYPD") on matters pertaining to counterterrorism, intelligence and security, which I do without compensation. However, I did not participate in the planning for security at the RNC, nor was I asked for my advice on that matter at the time.

6. I was a member of the White House Commission on Aviation Safety and Security in 1996 and 1997, where I was involved in discussions regarding personal identification. From 1999 to 2000, I served as an advisor to the National Commission on Terrorism and since 2000, I have served as a member of the U.S. Comptroller General's Advisory Board.

7. I am also the Director of the National Transportation Security Center at the Mineta Transportation Institute at San Jose State University in California ("MTI"). MTI was selected as a national Center of Excellence by the U.S. Department of Transportation through a competitive process in 2002. Since 1997 I have directed MTI's continuing research on protecting surface transportation against terrorist attacks.

8. I serve as a Special Advisor to the International Chamber of Commerce and am a member the Advisory Board of their investigative arm, Commercial Crime Services. Over the years I have served as a consultant to or carried out assignments for a number of government agencies. Additionally, as part of its international project to create a global strategy to combat terrorism, in 2004, the Club of Madrid appointed me to lead their international working group on the role of intelligence in combating terrorism.

9. I am currently self-employed as a consultant, and I am also a member of the adjunct staff of the RAND Corporation, where I serve as Senior Advisor to the President of RAND.

10. I have a B.A. in Fine Arts and a Masters Degree in History, both from the University of California, Los Angeles. I also studied at the University of Guanajuato in Mexico and in the Department of Humanities at the University of San Carlos in Guatemala where I was a Fulbright Fellow and recipient of a second fellowship from the Organization of American States.

11. I have written and edited numerous articles, book chapters, and published research reports on terrorism, security, conflict and crime. Some of my works include: (i) author of *International Terrorism: A New Mode of Conflict* (1974); (ii) editor and co-author of *Terrorism and Personal Protection* (1984); (iii) co-editor and co-author of *Aviation Terrorism and Security* (1998); (iv) co-author of *The Fall of South Vietnam* (1976); (v) author of

Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves (2006); (vi) author of *Will Terrorism Go Nuclear* (2006); and (vii) co-editor and co-author of *The Long Shadow of 9/11: America's Response to Terrorism* (2011).

12. I have been qualified and served as an expert witness in two prior cases. In 1984, I served as an expert witness on behalf of the defendants in a civil dispute involving terrorism, which was argued before an International Chamber of Commerce Arbitration Court in Paris. In 2010, I served as an expert witness for the defendants, Credit Lyonnais and National Westminster Bank, in civil litigation involving the alleged financing of certain terrorist attacks currently being litigated in the United States District Court for the Eastern District of New York. *Strauss et al. v. Credit Lyonnais, S.A. et al.*, (E.D.N.Y. 06 Civ. 702)(DLI)(MDG).

13. In this case, I have been asked to serve as an expert on behalf of the defendants in the matter of *Schiller et al. v. the City of New York, et al.*, 04 Civ. 7922 (RJS)(JCF), and *The Consolidated RNC Cases*, (RJS)(JCF), currently pending in the United States District Court for the Southern District of New York. For the reasons set forth below, the NYPD's decision to fingerprint all RNC arrestees, given the information available to the NYPD at the time, was not just good police practice, but essential to safeguard New York City and everyone in it.

Materials Reviewed

14. In addition to the materials cited in this declaration, and in addition to those that I have read and authored over the past 39 years as an expert in my field, I specifically reviewed the redacted 600-page open-source materials which were prepared by the NYPD Department of Intelligence under the leadership of Deputy Commissioner David Cohen and

provided to the NYPD in preparation for the RNC, which I understand are being referred to as the "End-User Reports."

15. I also reviewed the deposition testimony of the NYPD's Chief of Department Joseph Esposito.

My Conclusions

16. First, extraordinary circumstances prevailed in New York City in 2004. The passage of nearly ten years since 9/11 without another significant terrorist attack on American soil (with the exception of Major Nidal Hasan's attack at Fort Hood) makes it easy to forget the level of apprehension that existed in the shadow of the 9/11 attacks and the riots that broke out at the 1999 World Trade Organization Conference in Seattle. In these circumstances, it was legitimate and appropriate to implement enhanced security procedures for the 2004 RNC.

17. Second, state-issued driver's licenses do not provide an adequate and reliable means of personal identification. I have been involved in discussions of personal identification as a member of the White House Commission on Aviation Safety and Security in 1996 and 1997. I also testified before the 9/11 Commission and observed the debate over national identification in the United States.

18. More recently, I have returned to this issue as part of my recent work on suggesting new approaches to aviation security. In my opinion, any "trusted traveler" or "registered traveler" program must include biometrically confirmed identity, such as fingerprinting. For similar reasons, the NYPD's effort to confirm the identity of anyone arrested at an RNC event through fingerprinting was, in my view, justified. I expand upon these opinions in the following paragraphs.

The NYPD Was Presented with An Extraordinary Security Problem in 2004.

19. It was completely reasonable to impose the enhanced security measures that were imposed at the 2004 Republican National Convention in New York, including, specifically, fingerprinting RNC arrestees in order to verify their identity. Although it was only seven years ago, the atmosphere in 2004 was very different from that of today. The terrorist threat then was judged to be extremely high. The 2004 RNC took place less than 36 months after 9/11. During those 36 months, Al-Qaeda and its affiliates had continued a global terrorist campaign against those they deemed their enemies with major attacks in Indonesia, Pakistan, Kenya, Saudi Arabia, Tunisia, Morocco, and Turkey. Less than five months before the convention in New York, terrorists in Spain detonated a series of bombs on commuter trains, shortly before a Spanish national election, killing 191 people and injuring hundreds more. Additional terrorist plots had been uncovered in Europe and the United States.[1]

20. Historically, New York has been the subject of terrorist attacks and, since 9/11, the City has been the target of more terrorist plots than any other city. In 2003, terrorists reportedly planned to carry out a chemical attack on New York's subways. That same year, Lyman Faris, an Al-Qaeda operative, was arrested for reconnoitering the Brooklyn Bridge as a possible target for a terrorist attack, Uzair Paracha was arrested for assisting in possible attacks on gas stations, and Ahmed Omar Abu Ali was arrested for plotting to assassinate the President of the United States.

---

[1] To cite just one example only, just days before the 2004 RNC, in late August 2004, the NYPD arrested two individuals who were plotting to detonate a bomb at the Herald Square Subway station, just one block from Madison Square Garden – the epicenter of the 2004 RNC. The two plotters Shahawar Matin Siraj and James el-Shafay were charged with conspiring to blow up the subway station and were both later convicted. Mr. Siraj was a native of Pakistan who lived in Queens, New York and Mr. Elshafay was a United States citizen living on Staten Island.

21. At the end of 2003, the terrorist threat alert was raised to "orange" nationwide for the fifth time since the color-coded warning system had been implemented. It was raised again for the sixth time on August 1, 2004, just days before the RNC, when authorities discovered plans indicating financial institutions in New York City and Newark as possible terrorist targets. For the first time, the alert specified specific cities: New York, northern New Jersey, and Washington. And as noted above, in late August 2004, New York City police also arrested two individuals who planned to detonate a bomb in the Herald Square subway station, just one block away from Madison Square Garden.

22. At the same time that the U.S. invasion of Iraq in 2003 was spawning a ferocious insurgency led by Al-Qaeda that revitalized Al-Qaeda's recruiting efforts worldwide, it also provoked growing and passionate opposition in the United States. While protest often occurs at political conventions, it was also reasonable to anticipate a more confrontational atmosphere with a higher potential for violence at the 2004 RNC than at the Democratic National Convention, which preceded it. The Republicans were the party in power. The then President, George W. Bush, and his Vice-President, Dick Cheney, were reviled by many, to which one must add opponents of the Iraq War.

23. Both the 2004 Democratic National Convention in Boston and the 2004 RNC in New York, were the first national political conventions since 9/11. They were both designated as National Special Security Events ("NSSE"s).[2] This designation, created by

[2] The 2004 RNC was the 23rd such event, and the 13th since 9/11, to receive this designation. The NSSE designation means that special security procedures will be implemented to ensure a safe and secure environment for the general public, event participants, U.S. Secret Service protectees, and other dignitaries. NSSE operational plans include the use of physical security fencing, barricades, special access accreditation badges, K-9 teams, metal detectors, and explosive detection technologies. These are extraordinary security measures, equivalent to temporarily establishing airport-style security at a normally public location.

presidential directive in 1998, is given to events based on anticipated attendance by U.S. officials and foreign dignitaries, the size of the event, and its significance. The risk of a terrorist attack at a particular event increases as the number of participants at the event increases. In the case of the 2004 RNC, all the makings for a perfect storm were in place. The historical, political, and symbolic significance of the event, coupled with the attendance of large numbers of key American decision makers, as well as millions of everyday citizens, raised the risk levels to unprecedented highs.

Security Planning for the 2004 RNC, Including the NYPD, Had To Anticipate Trouble at the 2004 RNC.

24. In preparation for NSSEs, federal, state, and local authorities routinely study previous events, especially those where security was seen to have failed. In this regard, the 1999 World Trade Organization (WTO) Conference in Seattle would have been viewed as a precedent to be avoided.

25. Based on my review of the available literature regarding the "Battle of Seattle" and my discussions with law enforcement authorities, planning for protest demonstrations at the Seattle event, like planning for security, began months in advance. Agreements were negotiated between authorities and groups wishing to demonstrate, and permits were obtained for orderly marches. Other protest groups, however, sought confrontation aimed at disrupting the meeting and "direct action" -- meaning more than merely breaking the law by failure to disperse or passive resistance. Direct action includes destruction of property. Indeed, some people appeared determined to go beyond even blocking intersections and other forms of civil disobedience, and carry out physical attacks on corporate properties.

26. Some protestors seized control of key intersections, effectively preventing delegates from getting to the conference site. With police unable to clear the streets, smaller

groups of activists -- mostly anarchists -- exploited the situation and began smashing windows of downtown stores. Some of the unlawful protestors tried, unsuccessfully, to stop the vandalism, others joined in the melee, setting dumpsters on fire in the streets and even joining in the destruction. Among radical groups, the "Battle of Seattle" was seen as a victory and a model for future direct action. Post-9/11 WTO meetings scheduled for Washington, D.C. were cancelled due to security concerns. Canceling the RNC was not an option.

27. Thus planning for security at the 2004 Republican National Convention had to anticipate efforts by large numbers of demonstrators to shut down traffic in New York, thereby effectively shutting down the convention itself, as was done in Seattle. Police also had to be prepared for tactics that would prevent them from clearing the streets, including physical resistance and the demonstrators' tactic of "swarming" those law enforcement officials attempting to make arrests. I have reviewed the End User Reports prepared by the NYPD prior to the RNC and produced in the connection with RNC litigations. Even without that intelligence, the NYPD should have anticipated large-scale "direct action." Armed with that intelligence, the NYPD would have been grossly negligent had they not. As the lessons of the "Battle of Seattle" dictated, if the NYPD were unable to keep New York City's streets and thoroughfares and sidewalks clear, they would run the risk that more aggressive elements among the protestors, protected by masses of protestors, would launch direct attacks on property. Crowd psychology could prompt others to join in -- all of this against a backdrop of concern about a terrorist attack.

28. The NYPD open source intelligence gathering confirmed that many people were coming to New York for the RNC. It also confirmed that some of those people wished to engage in lawful protest, but that others were coming to deliberately break the law. In

addition, the NYPD had developed intelligence that protestors were advised to not carry identification or to carry false identification.

29. Given these facts, it was fair to ask whether protest at the RNC could be routinely handled as any other small-scale protest, or if a different security regime was required, especially when it came to arrest procedures. Under these circumstances, the NYPD implemented a procedure which required those who were arrested in connection with RNC unlawful activity to be photographed and fingerprinted, so that their identity could be verified. Doing so was simply prudent security practice for a high-security event.

30. Indeed, based on my conversations with law enforcement officials, in California and a number of other states, when officers cite individuals -- even for routine traffic violations -- who do not have identification documents or whose identification documents are suspect, they take them to a police station where they are booked, photographed, and fingerprinted, as a matter of course. This is the only way to accurately confirm their true identity.

What It Means "To Identify" Someone

31. Contemporary society requires reliable forms of identification for a variety of purposes: (a) proof of citizenship; (b) voting; (c) access to Social Security and federal or state medical benefits; (d) foreign travel; (e) commercial transactions including banking, the use of credit cards, etc.; (f) purchasing a firearm; (g) consumption of alcohol or purchase of cigarettes; (h) operating a motor vehicle; (i) air travel; (j) access to government or commercial buildings, factories, restricted areas; and (k) certification in certain skills or sports – e.g., scuba-diving.

32. All of these activities, and many others, require some confirmation of identity. The need to be able "to identity" oneself also creates powerful incentives for the creation of false or counterfeit identification documents.

33. To identify someone means simply to ascertain that the person actually is who they say they are, and therefore entitled to perform whatever function for which some form of identification is required -- to vote, receive a benefit, get a passport, travel abroad, withdraw money, cash a check, pay without cash, drive a car, enter a building, use student facilities, board an airplane, and/or rent a tank of air at a dive shop. Operationally, it means to match someone with the documents he or she is carrying.

34. The United States relies primarily on state-issued identification in the form of a driver's license, although some states' driver's license-issuing bureaus also offer non-driver's an equivalent identity document. These documents are also routinely used to confirm identity in, for example, commercial transactions, air travel, and access to buildings. Until recently, a driver's license was accepted in lieu of a passport for travel from the United States to Canada or Mexico. That is no longer the case.

Why People Conceal Their True Identities and/or Steal Identities.

35. People have many reasons for concealing or altering their own identity, using fake identification, and/or stealing the identity of others. Fugitives from the law obviously do not want to reveal their real identity and be caught. They often change identities, frequently adopting aliases to confuse authorities. James "Whitey" Bulger, despite being on the FBI's most wanted list, evaded arrest for sixteen years, during which he used more than a dozen aliases. This is not an isolated case. Every year, long-term fugitives from the law, who have evaded capture with false identities, are discovered and arrested.

36. Active criminals also create aliases to confuse law enforcement. Those participating in credit card fraud and identity theft rings create identities to match personal information obtained through hacking or other means.

37. Individuals with criminal records or strings of driving violations that would make them ineligible to obtain a commercial driver's license create new "clean" identities. Those whose driver's licenses have been suspended create new identities in order to obtain new driver's licenses. Those under 21 years of age who want to drink alcohol may carry identification with an altered birth date or a completely fake identification with a new name. Illegal immigrants may acquire fake identification to show that they are citizens. People escaping debt obligations obtain fake identification to evade their financial responsibilities. Thieves may use fake employee identification to gain access to port facilities, warehouses, cargo ramps, office buildings filled with laptop computers, or other lucrative venues.

Driver's Licenses are the Most Common Form of Identification

38. Driver's licenses contain many of the basic ingredients of identification -- name, address, age, a photo of the holder. But, as a general form of identification, driver's licenses have many shortcomings.

39. Driver's licenses are issued by the fifty different states, plus the District of Colombia and various territories. The formats vary widely, and they did even more so in 2004. Different states also have different procedures and apply different levels of rigor in confirming the information provided by an applicant. Some states are notoriously lax. Some suffer high levels of corruption. Based on my review of the available literature, in 2003 alone, news media reported two dozen cases in 15 states in which bribery or lax security at Department of Motor

Vehicle offices had resulted in fraudulent issuance of thousands of drivers' licenses. Card-making equipment can easily be stolen.

40. Computer-savvy individuals are creating thousands (some assert millions) of fake drivers' licenses despite the holograms and other features that states now require to be put on driver's licenses to prevent counterfeits, (but which few did in 2004). Replica drivers' licenses, barely distinguishable from the real thing, can be purchased on the Internet. Forged drivers' licenses can be bought on the street.

The 9/11 Commission Conclusions and the Identity Debate

41. All 19 of the 9/11 hijackers were foreigners. All entered the country legally on temporary visas (tourist or study visas) although three had overstayed their visas. All of them obtained U.S. identification that was used for boarding their flights in the form of drivers' licenses or non-driver identity cards. Altogether, the 19 hijackers had 17 drivers' licenses (one in Arizona, at least two in California, and 14 in Florida, four of which were duplicates). In addition, they had 13 state-issued identifications -- drivers' license equivalents for non-drivers (five from Florida, one from Maryland, and seven from Virginia). All seven in Virginia were obtained fraudulently.[3] This is a total of 30 documents, but another source indicates that the 19 hijackers had a total of 63 drivers' licenses or state identity equivalents.[4]

42. Undoubtedly, these easily obtained documents enabled the terrorists to travel, rent cars, open bank accounts and carry out other activities in support of their plot. It is

---

[3] Janice L. Kephart, "Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security," *Journal of Homeland Security*, March 2007.

[4] Federation for American Immigration Reform, "Identity and Immigration Status of 9/11 Terrorists," www.fairus.org/site/PageServer?pagename=iic immigration issuecenterc582, citing Pittsburgh Post-Gazette, March 28, 2002; see also Robert Thibadeau, "Workshop on States Security: Identity, Authentication, Access Control -- Organization and Themes," http://rack1.ul.cs.cmu.edu/tw/states security/thibadeau.PDF.

believed that at least six, and probably 18 of the hijackers, presented these as identification when they boarded flights on the morning of September 11 -- at least three of these were the fraudulently acquired Virginia documents.

43. This led the 9/11 Commission to recommend that the "federal government should set standards for the issuance of birth certificates and sources of identification such as drivers licenses."[5]

44. Clearly, procedures for issuing drivers' licenses did not prevent fraud and the documents themselves were easy to counterfeit. For example, Florida's drivers' license, which accounted for 19 of the hijackers documents, contained only a photo and facsimile of the holder's signature, but no hologram and no biometric identifier. Based on the available literature, in 2005, more than 20 states were still using paper photos glued into license forms -- an easily manipulated or duplicated document.

There Are Several Kinds of "False" Driver's Licenses

45. Because a driver's license is the most commonly used form of identification, it is the most frequently falsified. "False" drivers' licenses fall into two general categories: authentic drivers' licenses which contain false information, and fake drivers' licenses.

46. Authentic drivers' licenses may be sold by corrupt state officials to individuals wishing to establish a new identity. Individuals also lie to state authorities when applying for a driver's license, providing false information or concealing true information about themselves. To obtain drivers' licenses, they may provide falsified documents such as birth certificates.

---

[5] *Final Report of the National Commission on Terrorist Attacks on the United States*, Washington, D.C.: Government Printing Office, 2004, p.390.

47. Instructions are available on the Internet on how to create aliases, obtain, and alter birth certificates or create other fake paperwork in order to get authentic driver's licenses.

48. A fundamental weakness in the issuance of drivers' licenses is that they rely on "breeder documents" to confirm the applicant's identity. Such documents typically include birth certificates, which are easily counterfeited. There are in the United States thousands of jurisdictions issuing birth certificates. Those jurisdictions, in turn, use over 6,000 different forms, and there is no easy way to confirm their authenticity. Instructions on the Internet tell readers how to obtain and alter a birth certificate, which can then be used to obtain an authentic driver's license.

49. Another common breeder document is a driver's license from another state. Some states' licenses are easier to replicate than others, and some states are less rigorous in confirming applications. Virginia, for example, was seen as a state where it was easy to obtain driver's licenses. This enables one to easily graduate from a state with a less rigorous system to one with a more rigorous system.

50. Experts in the field agree that biometrics are the only reliable way to confirm the identity of an individual. Facial recognition technology has been increasingly used to check drivers' licenses applications, and retroactively to check drivers' licenses. (It was not widely used in 2004.) However, it is not as good as fingerprinting, and can lead to false matches, which then have to be investigated, requiring resources and time.

51. A 2003 General Accounting Office study reported that GAO agents operating undercover in seven states and the District of Colombia, using fake identification documents, meant to be obviously recognizable as fakes, were nonetheless able to obtain drivers'

licenses in every jurisdiction. Even when authorities spotted problems with the phony documents, the fake paperwork was never confiscated and law enforcement was never notified. In some cases, the GAO agents merely left the office, fixed the documents, reapplied, often on the same day, and still managed to successfully obtain drivers' licenses.

52. In other cases, the undercover operatives used fake out-of-state drivers' licenses to get authentic driver's licenses in other states. Persistence paid off. Although sometimes turned down on their first try, the GAO team managed to get licenses in every jurisdiction where they tried.[6]

53. The problem continues. For example, in 2011, New York State investigators used facial recognition technology to uncover drivers who had obtained licenses under different names. Forty-six commercial drivers, including bus drivers in New York City, were arrested on a single day as part of the continuing investigation.

54. According to published reports, since New York began checking licenses using the facial recognition technology, more than 3,000 persons were identified as having two or more different drivers' licenses, of which more than 600 were arrested on felony charges. The adoption of facial recognition technology to scrub existing drivers' license records for multiple identities and prevent new fraudulent applications led to the discovery of over 5,000 cases of fraud in Illinois between 1997 and 2007, and over 2,000 cases in a single year in Indiana. A review of all of Nevada's drivers' licenses led to 30,000 investigations. This suggests that there may be millions of fraudulently obtained driver's licenses nationwide, solely on the basis of multiple identities in a single state. Facial recognition does not detect individuals using

---

[6] U.S. General Accounting Office, *Security Vulnerabilities Found in Driver's License Applications Process*, GAO-03-989RNI (Washington, D.C.: September 9, 2003).

counterfeit documents to obtain fraudulently a single driver's license, nor does it identify individuals who may have additional identities in other states.

55. In addition to authentic driver's licenses containing false information, fake or counterfeit drivers' licenses can also be obtained. These are available on the Internet and, although described as novelty items, are also promoted as authentic or real-looking with holograms and other confirming markers. The replica is clearly marked on the back that it is not a state document, but it can be re-laminated and used as an authentic document. Templates for state driver's licenses are also available on the Internet, allowing individuals to "photo-shop" their photo and individual information to produce convincing replicas.

56. Fake drivers' licenses can also be obtained from illegal street vendors in most cities. The locations where the vendors do business are as widely known as are the locales for prostitution or purchasing drugs. In Los Angeles, for example, there are 15 to 20 "mills" continuously producing fake identification documents and constantly moving to avoid police detection. They cater primarily to illegal aliens and are often operated by illegal aliens themselves. The documents they produce are very good, containing the state logo, real license numbers (chosen at random) and real holograms or a glittering facsimile of a hologram. The entire process, from approaching a runner on the street to receiving the complete set of documents, takes about two hours. A good quality California driver's license goes for about $50, but for $70, one may obtain a complete set of counterfeit documents including a Social Security card, an immigration card, and a driver's license. Although this is a technically-sophisticated organized crime, albeit a cottage level industry, prosecutors are reluctant to prosecute individual cardholders. The resources required, given the volume of the crime, are too extensive. When they can be apprehended, counterfeit producers are prosecuted.

57. Finally, individuals may also use various graphics programs and desktop publishing to create reasonable facsimiles of genuine documents. Computer savvy teenagers have provided this service for their classmates. Stolen and altered driver's licenses -- a combination of real and fake -- add to the population of false driver's licenses.

Digital Technology Has Facilitated the Fabrication of Counterfeit Documents

58. Readily available online instructions and templates of drivers' licenses, computer graphics, and high quality color printers, and laminating equipment have facilitated copying and altering authentic licenses and creating counterfeit documents. This technology was available in 2004. As a result, law enforcement faced in 2004 and continues to face a huge problem of fraud based upon convincing supporting documents (letters of credit, bearer bonds, shares, etc.), counterfeit goods (pharmaceuticals with packaging so convincing that legitimate companies find it hard to distinguish their product from the fakes), and false identification documents.

Fake or False Identification Documents Are Hard to Distinguish

59. Federal officials (Customs and Border Patrol, Transportation Security) receive training in the detection of fake or false identification documents. We do not know what level of performance they achieve, but news media reports indicate failures. For example, Whitey Bulger, mentioned previously, traveled by air and regularly crossed the border with false identification, despite being near the top of the FBI's most wanted list.

60. In fact, TSA officials (like most law enforcement officers) are not document experts. If they were to check drivers' licenses with 13 sources of light, they might be better able to detect counterfeit documents, but that would be overly time consuming. (TSA is just now putting out a procurement notice to acquire counterfeit-detection technology.)

61. Police receive minimal training in document verification, usually only at the police academy. What they learn comes from on-the-job experience. Police training manuals have to be frequently revised to keep up with new techniques. Local police may be familiar with the drivers' licenses of their own state but less familiar with the myriad of drivers' licenses issued by other states.

Reliable Identification Requires Biometric Confirmation

62. Accordingly, reliable identification requires some form of biometric confirmation, fingerprinting being the most common. This is a well-established principle, which is why we see the increasing application of biometrics not only in controlling access to sensitive areas, but even in ordinary commercial transactions, for example, requiring a thumb print to notarize certain documents or to cash a check or even to enter an ordinary office building. Where these technologies are retroactively applied to identify fraudulent identification, such as New York State's employment of facial recognition technology to detect those with multiple driver's licenses, it underscores the weakness of mere photographs.

Conclusion

63. Putting all of this into the context of the 2004 Republican National Convention, I can say that the NYPD was well justified in expecting large numbers of individuals from across the country to descend on New York City for the 2004 RNC. It was also reasonable, given the open source materials, to expect that some percentage of those people would: (i) be coming with the specific intent to break the law; (ii) be carrying false or fake identification; and/or (iii) be carrying no identification whatsoever. Given the prevalence of false identification documents such as licenses (as well as the fact that everyday NYPD police officers would not be able to assess the authenticity of those documents), the NYPD's

implementation of a procedure to verify the identity of RNC arrestees through fingerprinting was reasonable and justified under all the circumstances. Thus, in my expert opinion, the NYPD's adoption of a procedure during the RNC that required biometric verification of identity -- through fingerprinting in this case -- was not merely reasonable and justified, but essential as well.

BRIAN M. JENKINS

Dated: New York, New York
October 3, 2011